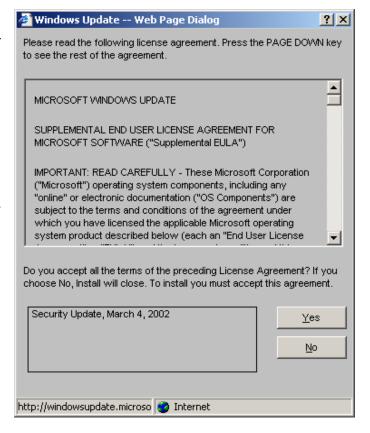Security Quickie 15 – Cross-site Referencing and Installations

The use of cross-site referencing is becoming more and more common on the Internet. It's a great way for advertising services and products with pop-up windows, and can also give the user access to sites they might not find during a normal search for resources. Unfortunately, vendors or malicious persons can also utilize cross-site referencing to install programs, product demos, or unwanted services onto unwary user's machines.

When you are browsing a website and looking for product updates or patches, the website can attempt to install such things for you quite readily. However, other cross-referenced sites might also attempt to install programs onto your machine, too. Be **certain** that what the site is attempting to install is exactly what you want to install. Do not trust sites blindly – they may have rented out advertising space or links to other sites or services. Check the pop-up installation document very carefully before clicking "Yes"!

An unauthorized installation might give out confidential or system information, open an insecure connection to an unknown, untrusted, or malicious source, or even install a backdoor into your system. If you do accidentally install something you did not intend to, contact your departmental Desktop Support Staff immediately. The Internet is a wondrous means of finding information and new programs, but use caution when installing things from the Internet – an unwanted or malicious program can also easily find **you**.